Which major legal concerns in future e-health?

Poullet, Yves; Herveg, Jean

Published in:
The Information Society : Innovation, Legitimacy, Ethics and Democracy in Honor of Professor Jacques Berleur s.j.

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

Which Major Legal Concerns in future e-Health ?

Jean Herveg, Yves Poullet
University of Namur (Belgium)
Faculty of Law – Research Centre for Computer and Law
jean.herveg@fundp.ac.be, yves.poullet@fundp.ac.be
http://www.crid.be

Abstract: e-Health Policy faces a radical change of perspective in the development of new e-Health projects. Indeed these projects are no longer conceived as simple answers to well-identified and specific needs. Today they are part of an Infrastructure Policy that aims at the establishment and the operation of real information highways in healthcare. This paper tests the creation of these highways against four validity criteria: necessity, transparency, security and confidentiality, and quality.

Keywords: e-Health, Health Telematic , Infrastructure, Data Protection, European Law

Introduction

1. e-Health is characterised by the use of Information and Communication Technologies in healthcare. These technologies have been used in healthcare in many ways for many years.

Using a first approach, e-Health is based on a large range of products dedicated to the management and the exploitation of information in healthcare. These products not only involve the software available in computers (1). There are as many products as there are types of information to manage and there are as many products as there are applications for which they are created. Information involves patients as well as the health practitioners, and information may be relative to all aspects of all activities

1 For example, they also include software in medical devices.

Please use the following format when citing this chapter:

Herveg, J., Poullet, Y., 2007, in IFIP International Federation for Information Processing, Volume 233, The Information Society: Innovations, Legitimacy, Ethics and Democracy, eds. P. Goujon, Lavelle, S., Duquenoy, P., Kimppa, K., Laurent, V., (Boston: Springer), pp. 159–170.

involved in healthcare - such as the provision of healthcare, its organisation, control, public or private funding, development of new medical devices or medicaments, as well as scientific research. The best-known products are electronic medical records. The development of e-Health is even more critical since, for decades, there have been more and more accurate medical information available concerning the patient in an individual or a collective approach. Scientific progress includes blood analysis, genetic engineering, medical imaging, etc. At the same time, medical treatments are improving and tend to be less and less invasive.

Using a second approach, e-Health is growing because it is based on telematic infrastructures, notably the Internet or private telematic networks. The exploitation of these infrastructures in healthcare aims at improving the circulation of information to the benefit of all the actors of healthcare, such as practitioners, patients, researchers (whether from university, public or private research centres, pharmaceutical or medical devices industries, etc.), public or private bodies participating to the funding of healthcare and the quality control of healthcare services, etc. These telecommunication infrastructures provide the practitioners with the ability to collaborate through a network and to use, share or offer, special e-Health products and services. Therefore new platforms are created in view of managing these networks. Logically, in this context, beyond information websites in healthcare, these networks give the opportunity to new services such as telemedicine applications, ambulatory devices with telecommunication functions, e-Prescription, and all the other applications using new Information and Communication Technologies in order to provide assistance tools to medical prevention, diagnosis, treatment, monitoring and lifestyle. With respect to this, new tools appear such as Information and Communication technologies implants that allow better tele-monitoring or even efficient and effective telemedicine insofar they allow direct medical intervention on the human being through implant to be considered as terminal. The patient is definitively entering into the circle of health telematic networks.

2. These new e-Health products and services are relatively well-known today even if all their technical and legal aspects are not fully under control[2]. However, e-Health now faces a radical change of perspective. Indeed, so far, the creation of a telematic network or infrastructure was based on a specific need : the development of a new product or service in healthcare. But, today, telematic networks or infrastructure are conceived without direct reference to specified purposes. They are created in view of permitting the achievement of future purposes that are to be defined in a next step. These telematic networks represent a purpose in themselves. They are like highways for vehicles, or like infrastructures for gas, electricity or telephone. These new telematic networks or infrastructures are to the products and services in healthcare what pylons and antennae are to telephone products and services. We currently witness the birth of new but real information highways in healthcare in their uttermost complete vision.

In this context, e-Health projects aim to create telematic networks or infrastructure at local, regional, national, European, international, or even worldwide

2 Especially in the case of international aspects.

level. The establishment and the operation of these networks or infrastructures are beyond the usual sphere of influence of traditional healthcare actors, and far beyond their traditional activities. Indeed, these networks involve more and more technicians, intermediaries, and many other actors such as public and private bodies participating to public health policy and social security policy. Many motivations may explain the creation of these networks e.g. in terms of public health, patient involvement in healthcare, healthcare funding and control of the quality, scientific research, discovery of new medicaments or medical devices. These new telematic networks or infrastructures are articulated around the information relative to all healthcare actors, e-Health products and services and their special infrastructures.

But, once more, the difference with these new telematic networks or infrastructure, is that their novelty lies in the permanence of their structure regarding their present and future exploitations. The opportunity to create such infrastructure is not evaluated anymore in view of a single specific purpose to be achieved. Their opportunity is measured in an abstract way regarding categories of future purposes for which content will be defined later. There is a radical change particularly as regards the required precision and materiality to assess the purposes of telematic infrastructures and their future exploitations.

In other words, these new telematic networks are information systems composed of two levels. The first level is the infrastructure (generally including shared data bases through the collection and processing of personal data – such as identification registries of patients and practitioners). The second level is the future purposes to be achieved by means of the infrastructure. Therefore these projects are in fact part of a policy aiming to create telematic infrastructures in healthcare. They also express a move from vertical organisations in healthcare to abstract, horizontal and transversal approaches in a first step and then specific and vertical approaches in a second step. The mere existence of these new telematic infrastructures in healthcare will enable shared databases, and imply the identification of practitioners and patients through special dedicated registries, etc. Eventually, these networks will deeply modify the organisation of healthcare. Furthermore, all actors in healthcare are involved including healthcare practitioners, social security and public health bodies, laboratories, patients, etc.

It is not possible to cover all the legal issues raised by these new information highways in this contribution. But it seems useful to analyse them according tofour criteria : (I) necessity, (II) transparency, (III) security and confidentiality, and (IV) quality.

I. Necessity

3. When one wishes to create information highways in healthcare, does one need to consider the necessity e-Health? Should the infrastructure be necessary to justify its creation and operation? From an ethical viewpoint, the question of the necessity to invest in this kind of infrastructure is quite mandatory since public and private resources are limited in healthcare. Logically, the creation of such information highways should correspond to real but imperative social needs. In this respect,

necessity should be assessed through multidisciplinary and rigorous experimental studies. In law, the notion of necessity may appear in different ways when creating and operating these new infrastructures in healthcare.

4. The notion of necessity may appear when the infrastructure is considered through the prism of the protection of the rights and liberties and especially regarding the right to respect for private life ([3]). Indeed, if a telematic infrastructure in healthcare and its operation may be viewed as an interference ([4]) by a public authority with the exercise of this right ([5]), this interference, according to article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and according to article 7 of the European Chart of Fundamental Rights, should be in accordance with the law[6] and should be, in a democratic society, necessary [7] to "*(...) the economic well-being of the country (...) for the protection of health (...) for the protection of the rights and freedoms of others.*" Furthermore the right to respect for private life may induce the (positive) obligation for the Member State to adopt appropriate measures to ensure the respect for private life in the sphere of the relations of individuals between themselves[8]. This obligation could lead to the necessity to regulate private infrastructures in healthcare. In determining whether or not such positive obligation exists, regard must be had to the fair balance which has to be struck between the interest of the infrastructure and the interests of the individuals, without prejudice of the margin of appreciation to be accorded to the competent national authority[9].

5. The notion of necessity appears also when telematic infrastructures are considered through the norms applicable to the processing of personal data. Indeed, the United Nations provide that a file containing personal data should only be created and used for specific and justified purposes [10]. In the same way, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement

3 European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8.

4 On the notion of interference : E.C.H.R., 27 August 1997, M.S. c. Sweden, §§ 33-35 ; 4 May 2000, Rotaru c. Romania, § 46.

5 On the notion of private life : E.C.H.R., 4 May 2000, Rotaru c. Romania, §§ 42- 43 ; 26 Feb. 2002, Pretty c. United-Kingdom, § 61 ; 24 June 2004, Von Hannover c. Germany, §§ 50-52, and 61.

6 Furthermore, the law must be accessible and foreseeable (on the latter, see : E.C.H.R., 4 May 2000, Rotaru c. Romania, § 55).

7 The necessity justifies the interference. The notion of necessity implies that the interference corresponds to an important social need and in particuliar that the interference should be proportionate with its legitimate purpose (E.C.H.R., 26 Feb. 2002, Pretty c. United-Kingdom, § 70). The Member States enjoy a margin of appreciation depending on the nature of the issues and the importance of the interests at stake (id.).

8 E.C.H.R., Von Hannover c. Germany, § 57.

9 On the positive obligation and its conditions : E.C.H.R., 7 Feb. 2002, Mikulic c. Croatia, § 58.

10 Guidelines concerning competurized personal data files, adopted by the General Assembly on 14 Dec. 1990 (resolution 45/95).Cf. also article 8 of the European Chart of Fundamental Rights.

of such data provides that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes[11]. To be legitimate or justified, the purpose must comply notably with the test of proportionality[12]. The later requires taking into account the necessity of the purpose of the infrastructure. In the same way, the notion of necessity appears in the principle of minimisation of the processing of personal data [13] which might be deduced from the data quality principle[14].

6. However these new telematic infrastructures cause a particular problem regarding the proportionality test. Indeed, since they constitute double-level information systems, the necessity of their creation and operating can only evaluated on an abstract base in the first place and on a real basis only after their exploitation. Put differently, their necessity will appear through their use. That is a risk to take into account at their beginning. This risk is not an impossible obstacle to the creation of these new infrastructures in healthcare. But it imposes a strengthening of the tools used to control their necessity, according to the safety precaution principle. In other words, these new infrastructures require special bodies and procedures in order to assess their necessity on a periodical base. With respect to this, this constraint is stronger with sensitive data like medical data.

II. Transparency

7. Should these new telematic infrastructures in healthcare be transparent? Before answering this question, we have to agree on the significance of the "transparency" concept.From a general point of view, transparency translates into the idea that the data flows generated by these telematic infrastructures should be known and accessible to all. They may not be secretly created but in a public way. In the same idea, their functioning should be transparent and under control. That transparency should be assessed in a collective way in order to control human activities, as well as in an individual way to ensure the respect for the rights and liberties of all. With respect to this, the characteristics of these new infrastructures in healthcare reduce their transparency regarding their operation since the later is not known with precision at the beginning but only after their exploitation. On the other hand and principally, the transparency of each data processing is not sufficient. The infrastructure has to be known in itself, and the multiple data flows it permits should be known as well. Regarding the latter, the necessity of a data flows' registry would

11 D. 95/46/CE, art. 6.1.b. The Directive provides that further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards (in the same way : Convention for the protection of individuals with regard to automatic processing of personal data, 28 Jan. 1981 (n° 108), art. 5.b).

12 The interests in presence are those of data subjects, data controllers, the society and interested third parties.

13 Regarding the Minimising Principle, see: Working Party, First Annual Report, 25 June 1997, WP 3, p. 15. In other words, one should minimise the processing of personal data.

14 As expressed in article 6.1.c. of Directive 95/46/EC.

have to be imposed beyond the simple information relative to each data flow considered on an individual base.

8. Regarding processing of personal data, transparency applies only to the processing and is mainly ensured by the information to be given to the data subject concerning the processing of his or her personal data, and by the right of access to his or her personal data that are processed [15], and by the notification of the data processing to the competent supervisory authority[16]. Concerning especially the information of the data subject, Directive 95/46/EC makes a difference if the personal data is or not obtained from the data subject [17] :

(a) the identity of the controller and of his representative, if any;
(b) the purposes of the processing for which the data are intended;
(c) any further information such as
- the recipients or categories of recipients of the data,
- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,
- the existence of the right of access to and the right to rectify the data concerning him or her in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

The duty to inform the data subject does not apply when the data have not been obtained from the data subject, in particular for processing for statistical purposes or for the purposes of historical or scientific research, whenever the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases, Member States shall provide appropriate safeguards[18].

The duty to inform the data subject involves the right of access to his/her personal data and in the right to obtain the rectification, erasure or blocking of data in case their processing does not comply with the provisions of Directive 95/46/EC, in particular because of the incomplete or inaccurate nature of the data. With respect to this, the organisation of the new telematic infrastructures should ease the exercise of the data subject's rights according to the principle of the reciprocity of advantages. When telematic infrastructures facilitate collection and processing of personal data, they should consequently provide data subjects with direct on-line access to their personal data and to data controllers and other bodies involved in the network.

When carrying special devices with telecommunication functions (such as health cards, Information and Communication Technologies implants, RFID implants, etc.), the data subject should control them. This control implies the transparency of their existence, the means of their operation, their information content, and the risks induced by the interruption of the service by the patient [19].

15 Directive 95/46/EC, art. 12.
16 Directive 95/46/EC, art. 18-21
17 Directive 95/46/EC, art. 10.
18 Id., art. 11.2.
19 See also art. 4.2. of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

The creation of these new telematic infrastructures raises another question. Who is globally in charge of the infrastructure, independently of the determination of the data controller for the personal data processing ? The solution to this question should not be delegated as such to jurisdictions. Independently from the determination of data controllers, the person in charge of the network, "the network controller", should be clearly identified. Indeed, only the conception and the quality of the network permit to consider the risks relative to the different data processing.

9. When the new telematic infrastructures open the door to new services of the information society[20], these latter must comply with special requirements in terms of transparency. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') provides special rules relative to additional general information to be provided[21], commercial communications[22] including unsolicited commercial communication[23] from regulated professions[24]. The Directive provides special rules relative to the information to be provided for the conclusion of contracts by electronic means[25] and for the placing of orders[26].

III. Security and Confidentiality

10. The security and confidentiality of information highways in healthcare are certainly more easy notions to understand. These requirements envisage or encompasse both levels of the information system. The infrastructure must be secure and stable. It should ensure the security and the confidentiality of the data processing performed in the framework of the second level.

Regarding the processing of personal data occurring at both levels, confidentiality implies that any person acting under the authority of the controller or of the processor, including the processor him or herself, who has access to personal data, must not process them except on instructions from the controller, unless s/he is

20 As defined in art. 1.2 of Directive 98/34/EC.
21 Directive 2000/31/EC, art. 5. These information concern mainly the identification and the localisation of the service provider.
22 Directive 2000/31/EC, art. 6.
23 Directive 2000/31/EC, art. 7.
24 Directive 2000/31/EC, art. 8. The use of commercial communications which are part of, or constitute, an information society service provided by a member of a regulated profession is permitted subject to compliance with the professional rules regarding, in particular, the independence, dignity and honour of the profession, professional secrecy and fairness towards clients and other members of the profession.
25 Directive 2000/31/EC, art. 10. These information concern the technical steps to follow to conclude the contract, the storage of the contract, the possibility to identify and correct errors, the languages offered for the conclusion of the contract. In the same way, contractual terms and general conditions must be made available in a way that allows him to store and reproduce them (there are exceptions for contract concluded exclusively by exchange of email or by mean of by equivalent individual communications).
26 Directive 2000/31/EC, art. 11. The service provider has to acknowledge the receipt of the recipient's order without undue delay and by electronic means.

required to do so by law[27]. Security implies that the data controller, also and in due cooperation with the so called "network controller", must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing[28]. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected[29] When processing is carried out on one's behalf, the data controller has to choose a processor[30] that provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures[31] It may seem difficult to comply with these constraints, especially when these telematic infrastructures imply the intervention of providers that are not subject to medical deontology or medical secrecy. Sometimes, the creation and the operation of these infrastructures may oppose traditional rules relative to medical secrecy. But information society technologies may provide many solutions to these problems. Directive 2002/58/EC provides rules concerning the security and the confidentiality of electronic communications but unfortunately only for infrastructures open to the public and accessible to him or her[32].

11. Concerning new information society services achieved through these new telematic infrastructures, Directive 2000/31/EC aims to ensure some legal certainty and consumer confidence[33] notably by regulating certain legal aspects of the conclusion of contracts by electronic means, when other Directives provides consumers with some protection[34]. The new products and services that could be

27 Directive 95/46/EC, art. 16.
28 See also art. 4.2 of Directive 2002/58/EC.
29 Directive 95/46/EC, art. 17.1.
30 Directive 95/46/EC, art. 17.1.
31 The notion of processor is different from the notion of data controller. The processor processes personal data in the strict framework of the mission determined by the data controller. He may not use the personal data for his own purposes. He must obey to strict confidentiality duties. His choice must be based on qualitative criteria. The notion of processor is very important and useful in the context of telematic infrastructures and networks in healthcare. This notion helps to qualify the function of several technical intermediaries (by example, an enterprise offering storage resources, or healthgrid platforms, or secondary providers in case of telemedicine).
32 Directive 95/46/EC, art. 17.2. Member States have the duty to identify data processing presenting particular risks and to check them prior their implementation (Directive 95/46/EC, art.20).
33 Directive 2000/31/EC, recital 7.
34 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market; Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use; Directive 97/7/EC on the protection of consumers in respect of distance contracts; Directive 1999/44/EC of the European Parliament and of the Council of 25 May 1999 on certain aspects of the sale of consumer goods and associated guarantees; Directive 2001/95 of the European Parliament and

offered through new telematic infrastructures in healthcare will strengthen the place of the patient in healthcare as a consumer, entitling him or her with all the rights (however, what about duties ?) subsequent to this qualification.

IV. Quality

12. Finally, the notion of the quality of the new telematic infrastructures in healthcare is essential. First, it raises the question about the availability of the products and services for practitioners and patients[35]. It raises the question of the technical quality of data transmission (data integrity). It also raises the question of the qualification and education of all the actors involved in the operation of the information system at both levels. Regarding the processing of personal data, the right of rectification and the right to oppose the processing participate indirectly to the data quality[36]. In terms of information society services, some special rules contribute to the quality of the system notably when they allow for the identification and the correction of input errors prior the placing of the order[37] and when they allow for the identification of the service provider (cf. *supra* n° 7).

Conclusions

13. The first age of e-Health is not yet fully implemented while the healthcare sector is already confronted with a radical change in its organisation. From a vertical implementation of new products and services, we now witness the creation of permanent telematic infrastructures and networks in healthcare. These new telematic infrastructures and networks raise concerns in terms of necessity, transparency, security and confidentiality, and quality. These infrastructures and networks are characterised by their permanency. We will have to evaluate their validity "*a posteriori*" and on a periodical base. The evaluation should take into account the interests of the society, the actors of healthcare, the patients, and citizens. In order to stimulate the acceptance of such information systems and improve their transparency, it seems opportune to implement clearly identified landmarks (bodies and procedures) in their creation and functioning by creating what Pierre Trudel qualifies as "trust circles". That is, in the context of these networks and through transparent regulatory means (including self-regulatory means), restricting the people authorised to act on and to gain access to certain resources that are present through

of the Council of 3 December 2001 on general product safety; Council directive 85/374/CE of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products as modified by Directive 1999/34/CE of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.
35 Directive 95/46/EC, art. 6.1.c and d.
36 See also art. 14 of Directive 2002/58/EC, concerning technical features and standardisation.
37 Directive 2000/31/EC, art. 10.1.c and art. 11.2.

the infrastructure. In Belgium, the Federal Be-Health Project represents a very good example of such evolution in the organisation of Public Health. This project aims to offer both a public platform and e-Health products and services to the benefit of practitioners and patients.

But one should not forget that healthcare cannot be reduced to machines, devices or informatics. First of all, healthcare is a liberal art. As such, it is not completely subject to rationalisation and to the use of information systems even if their quality and advantages are not questionable. Medicine is a combination of personal skills and knowledge. "Chance" has always been an important factor regarding the progress of medical knowledge. We should be very careful not to trust all our medical knowledge in machines and not to put all our money in it. We should also focus on the education of human-minded practitioners. Otherwise, we could forget how to progress and how to challenge established knowledge in order to progress. Information and Communication Technologies in healthcare are a challenge, more than ever, for both the worst and the best. We should go on trying to exploit the best of these technologies.

References

BENNETT, B. (ed.), *e-Health Business and Transactional Law*, Washington, BNA Books, 2002, 734 p.

BOULANGER, M.-H., de TERWANGNE, C., LEONARD, Th., LOUVEAUX, S., MOREAU, D. & POULLET, Y., " La protection des données à caractère personnel en droit européen ", Bruxelles, Larcier, *Journal des Tribunaux de Droit Européen.*, 1997, p. 121 et s. (en trois parties)

CALLENS, S. (ed.), *e-Health and the Law*, The Hague, Kluwer Law International, 2003, 183 p.

CHABERT-PELTAT, C., " La télémédecine ", Paris, *Revue Alain Bensoussan – Droit des Technologies Avancées*, 1999, n° 6/3-4, pp. 117-138.

Commission nationale de l'informatique et des libertés (CNIL-France), Délibération n° 97-049 du 24 juin 1997 portant avis sur la mise en œuvre à titre expérimental d'un réseau de télémédecine sur Internet entre le Centre hospitalier d'Annecy et certains médecins de ville, Paris, *Revue Alain Bensoussan – Droit des Technologies Avancées*, 1999, n° 6/3-4, pp. 169-172.

FLEISHER, L.D. & DECHENE, J.C., *Telemedicine and e-Health Law*, Law Journal Press, 2005.

HERVEG, J., " HealthGRID from a Legal Point of View ", in *From GRID to HEALTHGRID*, IOS Publications, Studies in Health Technology and Informatics, 2005, Volume 112, part 5, pp. 312-318.

HERVEG, J., VAN GYSEGHEM, J.-M. & de TERWANGNE, C., *GRID-enabled medical simulation services and European Law*, Final Report on all the Legal Issues related to Running GRID Medical Services, European Research contract IST-2001-37153-GEMSS, 29 February 2005, 341 p.

IAKOVIDIS I., WILSON, P., Healy J.-Cl., *E-Health: Current Situation and Examples of Implemented and Beneficial E-Health Applications*, IOS Press, Studies in Health Technology and Informatics, 2004, Volume 100, 249 p.

KAPLAN, G. & Mc FARQUHAR, E., *e-Health Law Manual*, New-York, Aspen Publishers, 2003.

RIENHOFF, O., LASKE, C., VAN EECKE, P., WENZLAFF, P. & PICCOLO, U., *A Legal Framework for Security in European Health Care Telematics*, Amsterdam, IOS Press, Studies in Health Technology and Informatics, vol. 74, 2000, 202 p.

RODRIGUES, R.J., WILSON, P. & SCHANZ, S.J., The Regulation of Privacy and Data Protection in the Use of Electronic Health Information, An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-Identifiable Health Databases, Pan American Health Information, World Health Organization, 2001, 217 p.

ROGER-FRANCE, Fr., " Informations de santé, télématique et télémédecine, Perspectives d'ensemble à l'horizon 2000 ", *Journal de réflexion sur l'informatique*, 1994, n° 30, pp. 7-9.

SILBER, D., *The case for eHealth*, Maastricht, Institut Européen d'Administration Publique (ed.), 2003, 32 p.

STANBERRY, B., *The Legal and Ethical Aspects of Telemedicine*, London, Royal Society of Medicine Press, 1998, 172 p.

VAN EECKE, P., "Electronic Health Care Services and the e-Commerce Directive", in *A Decade of Research @ the Crossroads of Law and ICT*, Gent, Larcier, 2001, pp. 365-379.

WILSON, P., LEITNER, Chr. & MOUSSALI, A., *Mapping the Potential of eHealth, Empowering the citizen through eHealth tools and services*, Maastricht, European Institute of Public Administration (ed.), 2004, 52 p.